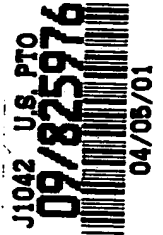


대한민국 특허청

KOREAN INDUSTRIAL
PROPERTY OFFICE



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Industrial
Property Office.

출원번호 :
Application Number

특허출원 2000년 제 60854 호

출원년월일 :
Date of Application

2000년 10월 17일

CERTIFIED COPY OF
PRIORITY DOCUMENT

출원인 :
Applicant(s)

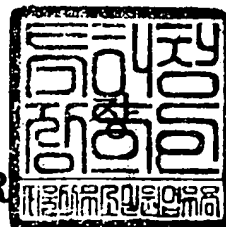
학교법인 한국정보통신학원



2000 년 12 월 13 일

특 허 청

COMMISSIONER



| | |
|------------|---|
| 【서류명】 | 특허출원서 |
| 【권리구분】 | 특허 |
| 【수신처】 | 특허청장 |
| 【참조번호】 | 0001 |
| 【제출일자】 | 2000. 10. 17 |
| 【발명의 명칭】 | 계산적 디피-헬만 가정에 가반하는 안전성 증명 가능한 공개키 암호화 방법 |
| 【발명의 영문명칭】 | PROVABLY SECURE PUBLIC KEY ENCRYPTION SCHEME BASED-ON COMPUTATIONAL DIFFIE-HELLMAN ASSUMPTION |
| 【출원인】 | |
| 【명칭】 | 학교법인 한국정보통신학원 |
| 【출원인코드】 | 2-1999-038195-0 |
| 【대리인】 | |
| 【성명】 | 장성구 |
| 【대리인코드】 | 9-1998-000514-8 |
| 【포괄위임등록번호】 | 2000-005740-6 |
| 【대리인】 | |
| 【성명】 | 이철희 |
| 【대리인코드】 | 9-1998-000480-5 |
| 【포괄위임등록번호】 | 2000-005742-1 |
| 【발명자】 | |
| 【성명의 국문표기】 | 백준상 |
| 【성명의 영문표기】 | BAEK, Jonsang |
| 【주민등록번호】 | 731205-1932420 |
| 【우편번호】 | 430-032 |
| 【주소】 | 경기도 안양시 만안구 박달2동 85 우성아파트 106-109 |
| 【국적】 | KR |
| 【발명자】 | |
| 【성명의 국문표기】 | 이병천 |
| 【성명의 영문표기】 | LEE, Byoungcheon |
| 【주민등록번호】 | 640310-1400816 |
| 【우편번호】 | 302-210 |
| 【주소】 | 대전광역시 서구 복수동 282 삼익목화아파트 106-2007 |
| 【국적】 | KR |

【발명자】

【성명의 국문표기】

김광조

【성명의 영문표기】

KIM, Kwangjo

【주민등록번호】

560410-1347622

【우편번호】

302-120

주소 지역 번호【주소】

대전광역시 서구 둔산동 삼성한마루아파트 7-1406

【국적】

KR

SCHEME BASED ON【심사청구】

청구

【조기공개】

신청

【취지】

특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구, 특허법 제64조의 규정에 의한 출원공개를 신청합니다. 대리인
 장성구 (인) 대리인
 이철희 (인)

【수수료】

【기본출원료】

17 면 29,000 원

【가산출원료】

0 면 0 원

【우선권주장료】

0 건 0 원

【심사청구료】

4 항 237,000 원

【합계】

266,000 원

【감면사유】

학교

【감면후 수수료】

133,000 원

【첨부서류】

1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 적응적 암호문 선택공격에 대한 안전성이 증명 가능한 공개키 암호 방법에 관한 것으로, 본 발명의 공개키 암호화 방법은 (a) 수신측에서, 변수(p, q, g)(여기서, p 는 길이 k 를 갖는 충분히 큰 소수이고, q 는 $p-1$ 을 나누는 충분히 큰 소수이며, g 는 곱셈군 Z_p^* 에서 위수가 q 인 생성원)를 공개키 파라미터로서 선택하는 단계; (b) 수신측에서, 제 1 해쉬 함수 H (여기서, $H: \{0, 1\}^* \rightarrow Z_q$)와 제 2 해쉬함수 G (여기서, $G: Z_p^* \rightarrow \{0, 1\}^*$)를 선택하여 공개하는 단계; (c) 수신측에서, 상기 선택된 공개키 파라미터(p, q, g)를 바탕으로 $x \in Z_q$ 를 만족하는 x 를 선택하여 비밀키로서 보관하고 $X \in Z_p^*$ 를 만족하는 공개키 X 를 생성하여 각각의 공개키 파라미터와 공개키(p, q, g 및 X)를 공개하는 단계; (d) 송신측에서, 상기 생성된 공개키 X 를 이용하여 상기 평문 m 을 암호화하여 암호문(α, β)을 생성하는 단계; (e) 수신측에서, 상기 송신측으로부터 전송된 암호문(α, β)에 대하여 유효성을 검증하는 단계; (f) 수신측에서, 유효성이 검증된 상기 암호문(α, β)을 상기 비밀키 x 를 이용하여 평문으로 복호화하는 단계를 포함한다.

본 발명은 종래의 결정적 디피-헬만 가정에 비하여 약한 가정으로 알려진 계산적 디피-헬만 가정에 안전성을 기반하고 있고, 암호문의 길이가 짧아져서 효율성이 높아지는 특징이 있다.

【대표도】

도 3

【명세서】

【발명의 명칭】

계산적 디피-헬만 가정에 기반하는 안전성 증명 가능한 공개키 암호화 방법{PROVABLY SECURE PUBLIC KEY ENCRYPTION SCHEME BASED ON COMPUTATIONAL DIFFIE-HELLMAN ASSUMPTION}

【도면의 간단한 설명】

도 1은 일반적인 공개키 암호 시스템의 블록 구성도,

도 2는 본 발명에 따른 적응적 암호문 선택 공격에 대한 안전성이 증명 가능한 공개키 암호화 방법을 구현하는 데 적합한 시스템의 블록 구성도,

도 3은 도 2에 도시된 적응적 암호문 선택 공격에 대한 안전성이 증명 가능한 공개키 암호화 방법의 동작을 설명하는 흐름도.

<도면의 주요부분에 대한 부호의 설명>

10, 100 : 암호화 장치

20, 200 : 복호화 장치

30, 300 : 공개키 디렉토리

400 : 인증 검사부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<7> 본 발명은 공개키 암호화 방법에 관한 것으로, 보다 상세하게는 적응적 암호문 선택공격에 안전한 암호화 방법에 관한 것이다.

<8> 최근 정보통신망의 발전과 더불어 다양한 정보가 네트워크를 통하여 교류되고 있다. 송신자가 전자 우편이나 전자 문서 전달 시스템 등을 통하여 귀중한 메시지를 전

달하고자 할 때, 통신로 상에서 의도한 수신자 이외의 제 3자가 이 귀중한 메시지에 대한 정보를 갈취하는 것을 방지하기 위해 메시지를 암호화하여 전달하게 된다. 이러한 암호화를 수행하기 위한 방법은 암호화와 복호화시 동일한 키를 사용하는 대칭키 암호화 방법과 암호화를 위한 키(공개키)와 복호화를 위한 키(비밀키)를 다르게 사용하는 공개키 암호화 방법이 있다.

- <9> 특히, 공개키 암호화 기법은 암호화를 위한 공개키와 복호화를 위한 비밀키를 달리 하여 사용하는 방법으로 비대칭적 암호화 기법이라고도 지칭된다. 즉 사용자가 자신의 공개키를 공개키 디렉토리에 공개하면 이 사용자에게 비밀성이 요구되는 메시지를 보내려는 다른 사용자는 공개된 공개키를 이용하여 메시지를 암호화하여 전송할 수 있다. 공개키로 암호화된 정보는 이에 대응하는 키, 즉 비밀키에 의해서만 복호화될 수 있기 때문에 메시지의 비밀성이 보장된다.
- <10> 도 1을 참조하면, 일반적인 공개키 암호 알고리즘을 사용하는 공개키 암호 시스템의 블록 구성도로서, 송신자측의 암호화 장치(10), 수신자측의 복호화 장치(20) 및 공개키 디렉토리(30)를 포함한다. 수신자측의 복호화 장치(20)는 수학적 역 변환에 의한 공개키와 개인키(또는 비밀키)를 연산하여 공개키는 모든 사람이 알 수 있는 공개키 디렉토리(30)에 공지하고, 개인키는 수신자측의 복호화 장치(20)에 비밀히 보관한다.
- <11> 송신자측의 암호화 장치(10)는 암호화하고자 하는 평문 메시지를 공개키 디렉토리(30)에 보관된 공개키를 이용하여 암호화한 후, 암호화된 암호문을 통신 채널(50)을 통하여 수신자측의 복호화 장치(20)로 전송한다. 수신자측의 복호화 장치(20)는 자신이 공개키 디렉토리(30)에 공개한 공개키와 대응되는 비밀키로 송신자로부터 제공된 암호문을 복호화하여 송신자측의 암호화 장치에서 전송한 원래의 평문 메시지를 복원한다.

<12> 그러나, 송신자측의 암호화 장치(10)와 수신자측의 복호화 장치(20)사이에서 암호문이 전송될 때, 암호문은 안전성이 보장되지 아니한 전송로(50)를 통하게 되므로 의도적으로 불순한 공격자에 의해 공격받을 수 있다. 이러한 공격에는 공격자가 단순히 암호내용을 감청하여 암호문으로부터 평문이나 비밀키에 관한 정보를 추출하는 수동 공격과 통신로에 공격에 용이한 정보를 삽입하여 해독하는 능동 공격이 있다.

<13> 능동 공격이 허용되는 상황에서, 공격자는 암호문에 대한 부분적인 정보(예를들면, 평문의 최하위 비트 값 등)에 관한 해독이 성립할 수 있으므로, 이에 대응하여 공개키 암호 시스템은 어의적 안전성(semantic security)을 보장하여야 한다.

<14> 그러나 대부분의 공개키 암호 시스템은 대수학적 성질을 가지고 있기 때문에, 예를 들어, 2개 암호문의 곱은 2개 평문의 합과 같다는 특성 때문에, 공격자가 능동 공격 방법 중 선별적인 암호문으로 공격을 시도하는 경우가 발생한다. 이와 같이, 공격자가 암호문(c)에 대한 정보(키 혹은 암호문에 상응하는 평문)를 얻기 위하여 암호문(c)과는 다르지만 암호문(c)과 관련이 있는 암호문(c')들에 대한 복호화를 요청하여 이루어지는 공격을 적응적 암호문 선택공격(Adaptive Chosen Ciphertext Attack : 이하 ACCA라고 함)

이라 지칭한다. 이 때 공격자는 암호문(c)를 직접 복호화할 수는 없다. 이런 ACCA에 대한 안전성을 보장하는 공개키 암호 시스템을 구성하는 것은 상당히 어려운 일로 분류되어 왔다.

<15> ACCA는 실제로 공개키 암호시스템에 대하여 가해질 수 있는 매우 강력한 공격중의 하나이다. 예전에는 공개키 암호시스템의 설계시 주로 평문의 내용을 효과적으로 숨기는 것에 주로 설계의 초점을 맞추었으나 최근에는 설계되는 공개키 암호 시스템들이 ACCA에 안전한가에 설계의 초점이 많이 맞추어지고 있는 실정이다. 하지만 ACCA에 어느 정도의

수준으로 안전성을 제공하는가에 따라 계산량의 증가도 가져오고, 메시지의 길이도 늘어나게 되는 경우가 대부분이다.

<16> ACCA에 안전한 공개키 암호시스템중의 하나는 1991년 라코프(Rackoff)와 사이몬(Simon) 등이 비대화형 영지식 증명법(non-interactive zero knowledge proof)을 이용한 기법이 제안되어 있다. 이 기법들은 공개키 암호시스템의 안전성에 관한 수학적인 증명은 제공하였지만 실용적이지 못하다는 평을 받았다.

<17> 이후 1993년 벨라레(Bellare)와 로가웨이(Rogaway)가 이상적인 해쉬함수를 가정하고 (이하, 랜덤 오라클 모델이라 함) RSA 가정을 기반으로 하고 있는 실용적이고 ACCA에 대한 안전성이 증명 가능한 공개키 암호화 기법을 제안하였다.

<18> 그리고 1999년 후지사키(Fujisaki)와 오카모토(Okamoto)는 랜덤 오라클 모델 하에서 결정적 디피-헬만 가정(decisional Diffie-Hellman assumption)에 기반하고 있고 ACCA에 대한 안전성이 증명 가능한 매우 효율적인 공개키 암호화 기법을 제안하였다. 결정적 디피-헬만 가정이란 공격자가 두 개의 확률분포 (g^x, g^y, R) 과 (g^x, g^y, g^{xy}) (여기서 R 은 일정 길이의 난수이며 R 과 g^{xy} 의 길이는 같다고 가정한다. 또한 g^x 와 g^y 의 값은 곱셈군 Z_p^* 상에서 계산된다)를 구별하는 확률이 무시할 수 있을 정도로 작다는 가정이다.

<19> 2000년 포앙셰발(Pointcheval)은 후지사키와 오카모토 공개키 암호화 기법의 기본 가정인 결정적 디피-헬만 가정보다 약한 가정이라고 알려진 계산적 디피-헬만 가정(computational Diffie-Hellman assumption)을 기반으로 하고, 랜덤 오라클 모델하에서 ACCA에 대한 안전성이 증명 가능한 공개키 암호화 기법을 제안하였다. 계산적 디피-헬만 가정이란 공격자에게 곱셈군

Z_p 상의 \mathcal{E}^* 와 \mathcal{E}' 의 두 값이 주어졌을 때, 공격자가 \mathcal{E}^* 를 계산할 확률이 무시할 수 있을 정도로 작다는 가정이다. 그러나 포앙쉐발의 공개키 암호화 기법의 한 가지 단점은 하나의 메시지를 암호화할 때 암호문의 길이가 보안 파라미터의 3배 정도로 늘어난다는 것이다.

<20> ACCA에 안전한 공개키 암호화 기법에서 공통적으로 채택하고 있는 방법은 공격자가 임의로 암호문을 변경할 수 없도록 암호문의 인증성을 제공하는 것이다. 송신자측의 암호화 장치는 수신자측 복호화 장치에서 생성되어 공개키 디렉토리에 공개된 공개키를 사용하여 암호화할 때 암호화하고자 하는 평문 또는 암호화된 암호문에 인증성을 보장해주는 특정한 구조를 가지고 있다. 통신 채널을 통해 암호화 장치로부터 전송된 암호문을 수신한 복호화 장치는 이 암호문에 들어 있는 특정 구조를 암호문을 복호화하기 전 또는 복호화한 후에 확인하는 절차를 수행하며, 그 결과 유효한 구조라고 판단될 때 평문을 최종적으로 받아들인다.

<21> 이는 ACCA에 안전한 공개키 암호화 기법의 전형적인 구조로, 종래의 공개키 암호화 기법과 비교할 때 암호화하는 과정은 비슷하나 복호화하는 과정에서 암호문의 유효성 확인 절차 또는 평문의 유효성 확인 절차를 더 포함하고 있다.

<22> 그러므로, ACCA에 대한 안전성이 증명 가능한 공개키 암호화 기법을 제공하는 것이 필요하다.

【발명이 이루고자 하는 기술적 과제】

<23> 본 발명은 전술한 공개키 암호화 기법들의 문제를 해결하고자 안출된 것으로, 본 발명은 결정적 디피-헬만 가정보다 약한 가정인 계산적 디피-헬만 가정에 기반하고 종래

의 기법보다 암호문의 길이가 짧으며 랜덤오라클 모델 하에서 ACCA에 대한 안전성이 증명 가능한 공개키 암호화 기법을 제공하는 것을 그 목적으로 한다.

<24> 상술한 목적을 달성하기 위한 본 발명에 따르는 ACCA에 안전한 공개키 암호화 방법은: (a) 수신측에서, 변수(p, q, g)(여기서, p 는 길이 k 를 갖는 충분히 큰 소수이고, q 는 $p-1$ 을 나누는 충분히 큰 소수이며, g 는 곱셈군 Z_p^* 에서 위수가 q 인 생성원)를 공개키 파라미터로서 선택하는 단계; (b) 수신측에서, 적응적 암호문 선택공격에 대하여 안정성을 보장하는 제 1 해쉬 함수 $H: \{0,1\}^* \rightarrow Z_q$ 와 계산적 디피-헬만 가정의 안정성을 보장하는 제 2 해쉬함수 $G: Z_p^* \rightarrow \{0,1\}^*$ 를 선택하여 공개하는 단계; (c) 수신측에서, 상기 선택된 공개키 파라미터(p, q, g)를 바탕으로 $x \in Z_q$ 를 만족하는 x 를 선택하여 비밀키로서 보관하고 $X \in Z_p^*$ 를 만족하는 공개키 X 를 생성하여 각각의 공개키 파라미터와 공개키(p, q, g 및 X)를 공개하는 단계; (d) 송신측에서, 상기 생성된 공개키 X 를 이용하여 상기 평문 m 을 암호화하여 암호문(α, β)을 생성하는 단계; (e) 수신측에서, 상기 송신측으로부터 전송된 암호문(α, β)에 대하여 유효성을 검증하는 단계; (f) 수신측에서, 유효성이 검증된 상기 암호문(α, β)을 상기 비밀키 x 를 이용하여 평문으로 복호화하는 단계를 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<25> 이하 본 발명은 첨부된 도면을 참조하여 다음과 같이 상세히 설명될 것이다.

<26> 도 2는 본 발명에 따른 공개키 암호화 기법의 개략적인 블록 구성도로서, 송신자측의 암호화 장치(100)와 수신자측의 복호화 장치(200) 및 공개키 디렉토리(300)를 포함한다. 또한, 복호화 장치(200)는 인증 검사부(400) 및 복호화부(450)를 포함한다.

- <27> 수신자측의 복호화부(450)는 충분히 큰 소수 p , q , 및 생성원 g 를 포함하는 공개 키 파라미터들을 생성한다. 또한, 복호화부(450)는 비밀키를 랜덤하게 생성하고, 이 값을 생성원 g 에 곱승하여 공개키를 생성함으로써, 공개키 및 비밀키 쌍을 생성한다. 공개키는 공개키 디렉토리(300)에 게시되고, 비밀키는 안전한 곳에 보관된다. 수신자측의 복호화부(450)에서 생성된 공개키는 송신자측의 암호화 장치(100)에서 평문메시지를 암호화하는데 사용되고, 비밀키는 암호화된 평문 메시지를 복호화하는데 사용된다.
- <28> 송신자측의 암호화 장치(100)는 랜덤 수 r 을 선택하여 평문 메시지를 암호화하여 생성된 암호문을 통신 채널(500)을 통하여 수신자측으로 전송한다.
- <29> 수신자측의 인증 검사부(400)는 도 1에 예시된 종래 기술의 공개키 암호화 기법에 암호문의 전송 도중 공격자에 의해 변조되었을 경우 그 변조 여부를 검사하는 기능을 수행하는 메시지 인증성 검사부분으로 사용된다. 보다 상세히 말해서, 인증 검사부(400)는 송신자측의 암호화 장치(100)로부터 전송된 암호화된 평문 메시지의 암호문을 복호화부(450)에서 복호화하기 전에 비밀키를 이용하여 암호문이 유효한지를 판단하고, 전송된 암호문이 유효한 경우에만, 복호화부(450)로 하여금 상술한 복호화를 수행하도록 한다.
- <30> 이하, 상술한 구성을 갖는 본 발명의 공개키 암호화 방법은 도 3의 흐름도를 참조하여 보다 상세히 설명될 것이다.
- <31> 먼저, 공개키 파라미터 선택 단계(500)에서, 수신측의 복호화부(450)는 공개키 파라미터, 즉, 충분히 큰 소수 p (여기서 p 의 길이는 k)와, $p-1$ 을 나누는 충분히 큰 소수 q 그리고 위수가 q 인 곱셈군 Z_p^* 의 생성원 g 를 공개키 파라미터로서 선택한다. 여기서 생성원이라는 것은 $g^0, g^1, g^2, \dots, g^{q-1}$ 이 Z_p^* 의 서로 다른 모든 원소가 되게하는 Z_p^* 상의 원소를 의미한다.

- <32> 그 다음 해쉬함수 선택 단계(510)에서, 복호화부(450)는 두 개의 해쉬 함수(랜덤 오라클) H (여기서, $H: \{0, 1\}^* \rightarrow Z_q$)와 G (여기서, $G: Z_p^* \rightarrow \{0, 1\}^*$)를 선택하여 공개한다.
- <33> 통상적으로, 해쉬 함수는 임의의 길이의 데이터를 입력으로 하여 정해진 길이의 출력값(예를 들면, 160 비트)을 내는 결정론적인 함수로서 예측 불가능한 난수성을 가짐으로써, 똑같은 해쉬 값을 출력하는 두개의 데이터를 찾아내기가 계산적으로 불가능하게 한다. 이러한 해쉬 함수 H 와 G 는 송신측과 수신측이 상호 공유하여야 하는 사전 공유된 시스템 파라미터로서, 암호문의 난수성을 보다 향상시키기 위하여 사용되며, MD5, SHA-1 등과 같이 공개된 암호학적 해쉬함수를 이용하여 구성한다.
- <34> 그 다음 공개키 생성 단계(520)에서, 복호화부(450)는 선택된 공개키 파라미터(p , q , g)를 바탕으로 $x \in Z_q$ 를 만족하는 x 를 선택한 후, x 는 비밀키로서 보관하고, 하기 수학식 1과 같이 $X \in Z_p^*$ 를 만족하는 공개키 X 를 계산하여 공개키 파라미터와 공개키(p , q , g 및 X)를 공개키 디렉토리(300)에 게시한다.

<35> 【수학식 1】

$$X = g^x$$

- <36> 그 다음 암호화 단계(530)에서, 송신측의 암호화 장치(100)는 ACCA에 대한 공격에 암호 시스템을 견딜 수 있게 하는 인증 코드(authentication code)의 역할을 하는 해쉬 함수 H , 길이 k_1 의 랜덤 스트링 r 과 계산적 디피-헬만 가정의 안전성을 보장하는 해쉬 함수 G , 수신측의 복호화부(450)에서 생성한 공개키 X 를 이용하여 전송하고자 하는 길이 k_0 (단, $k_0 + k_1 = k$ 이다)의 평문 m 의 암호문 (α, β) 를 하기 수학식 2와 같이 계산한다.

<37> 【수학식 2】

$$(\alpha, \beta) = (g^{H(m||r)}, G(X^{H(m||r)}) \oplus (m||r))$$

<38> 상술한 수학식 2로부터 알수 있는 바와 같이, 랜덤 오라클 G 를 $X^{H(m||r)}$ 에 적용함으로써 결정적 디피-헬만보다 약한 계산량적 가정인 계산적 디피-헬만 가정에 안전성을 기반하는 공개키 암호화 기법을 구성할 수 있고, 또한 메시지 m 에 랜덤 스트링 r 을 연접한 후 랜덤 오라클 H 를 적용하여 이를 g 에 역승함으로써 수신측에서 암호문의 인증성을 검사하여 ACCA에 대한 안전성을 제공할 수 있다. 이렇게 생성된 암호문(α , β)은 통신 채널(500)을 통하여 수신자측으로 전송된다.

<39> 그 다음 암호문 유효성 검증 단계(540)에서, 수신자측의 인증 검사부(400)는 송신자측의 암호화 장치(100)로부터 전송된 암호문(α , β)의 유효성을 검증하기 위하여, 암호문의 변수 α , β 와 비밀키 x 를 이용하여 다음과 같이 수학식 3을 계산한 후 하기 수학식 4가 성립하는 지를 판단한다.

<40> 【수학식 3】

$$t = G(\alpha^x) \oplus \beta$$

<41> 수학식 3에서, t 는 수신측에서 암호문 검증을 위하여 암호문(α , β)으로부터 계산해내는 검증값이다.

<42> 【수학식 4】

$$\alpha = g^{H(t)}$$

<43> 인증 검사부(400)에서의 인증 결과, 수학식 4가 성립하지 않는다면 송신자측의 암호화 장치(100)에서 전송된 암호문(α , β)이 유효하지 않은 것으로 판단하고, 암호문을 버리기 위하여 '리젝트(reject)'라는 메시지를 출력하고 송신측의 암호화 장치(100)에 대하여 암호문의 재전송을 요구한다.

<44> 그러나, 수학식 4의 성립이 확인되면 암호문 복호화 단계(550)로 진행하여, 복호화 부(450)에서 상술한 수학식 3의 검증값 t 에서 뒷부분에 연접된 k_1 길이의 난수 r 을 제거하고 k_0 길이의 평문 m 을 복원한다.

【발명의 효과】

<45> 본 발명에서는 랜덤 오라클(해쉬함수) G 를 $X^{H(m||r)}$ 에 적용함으로써 결정적 디피 헬만보다 약한 계산량적 가정인 계산적 디피-헬만 가정에 안전성을 기반하는 공개키 암호화 기법을 구성할 수 있고, 또한 메시지 m 에 랜덤 스트링 r 을 연접한 후 해쉬함수 H 를 적용하여 이를 g 에 멍승함으로써 복호화 과정에서 암호문의 인증성을 검사하여 ACCA에 대한 안전성을 제공할 수 있다. 또한, 본 발명에 따라 보안 파라미터 k 의 2배에 해당하는 암호문 길이를 얻음으로써 기존 포앙쉐발의 결과(암호문이 k 의 3배)와 비교할 때 암호문의 길이를 최적화 시킬 수 있다.

【특허청구범위】

【청구항 1】

전송하고자 하는 k_1 길이의 평문 m 을 암호화하는 암호화 장치와 암호문을 상기 평문 m 으로 복호화하는 복호화 장치로 구성되는 공개키 암호 시스템의 적응적 암호문 선택 공격에 안전한 공개키 암호화 방법에 있어서,

(a) 상기 복호화 장치에서, 변수(p, q, g)(여기서, p 는 길이 k 를 갖는 충분히 큰 소수이고, q 는 $p-1$ 을 나누는 충분히 큰 소수이며, g 는 곱셈군 Z_p^* 에서 위수가 q 인 생성원)를 공개키 파라미터로서 선택하는 단계;

(b) 상기 복호화 장치에서, 적응적 암호문 선택공격에 대하여 안정성을 보장하는 제 1 해쉬 함수 H (여기서, $H: \{0,1\}^* \rightarrow Z_q$)와 계산적 디피-헬만 가정의 안정성을 보장하는 제 2 해쉬함수 G (여기서, $G: Z_p^* \rightarrow \{0,1\}^*$)를 선택하여 공개하는 단계;

(c) 상기 복호화 장치에서, 상기 선택된 공개키 파라미터(p, q, g)를 바탕으로 $x \in Z_q$ 를 만족하는 x 를 선택하여 비밀키로서 보관하고 수학식 $[X=g^x]$ 을 만족하는 공개키 X 를 생성하여 각각의 공개키 파라미터와 공개키(p, q, g 및 X)를 공개하는 단계;

(d) 상기 암호화 장치에서, 상기 복호화 장치에서 생성된 공개키 X 를 이용하여 상기 평문 m 을 암호화하여 암호문(α, β)을 생성하는 단계;

(e) 상기 복호화 장치에서, 상기 암호화 장치로부터 전송된 암호문(α, β)에 대하여 유효성을 검증하는 단계;

(f) 상기 복호화 장치에서, 유효성이 검증된 상기 암호문(α, β)을 상기 비밀키 x

를 이용하여 평문으로 복호화하는 단계를 포함하는 것을 특징으로 하는 계산적 디피-헬만 가정에 기반하는 안전성이 증명가능한 공개키 암호화 방법.

【청구항 2】

제 1 항에 있어서, 상기 암호화 단계(d)에서, 상기 암호문(α, β)은 수학식 $[(\alpha, \beta) = (g^{H(m||r)}, G(X^{H(m||r)}) \oplus (m||r))]$ 을 이용하여 생성되며,

상기 수학식에서, r은 임의로 선택된 k_0 길이의 랜덤 스트링으로, $[k_0 + k_1 = k]$ 의 관계를 만족하는 것을 특징으로 하는 계산적 디피-헬만 가정에 기반하는 안전성이 증명가능한 공개키 암호화 방법.

【청구항 3】

제 2 항에 있어서, 상기 암호문의 유효성 검증 단계(e)는:

수학식 $[r = G(\alpha^s) \oplus \beta]$ 를 계산하여 상기 암호문의 변수 α 가 수학식 $[\alpha = g^{H(r)}]$ 을 만족하는지를 판단하는 단계를 구비하는 것을 특징으로 하는 계산적 디피-헬만 가정에 기반하는 안전성이 증명가능한 공개키 암호화 방법.

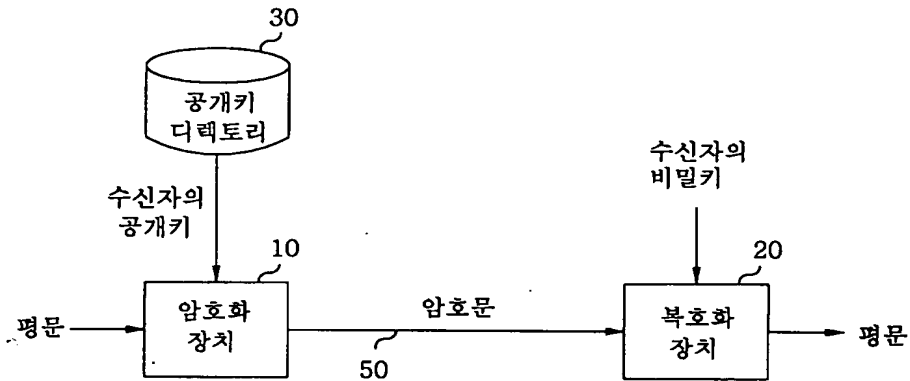
【청구항 4】

제 3 항에 있어서, 상기 암호문을 복호화하는 단계(f)는:

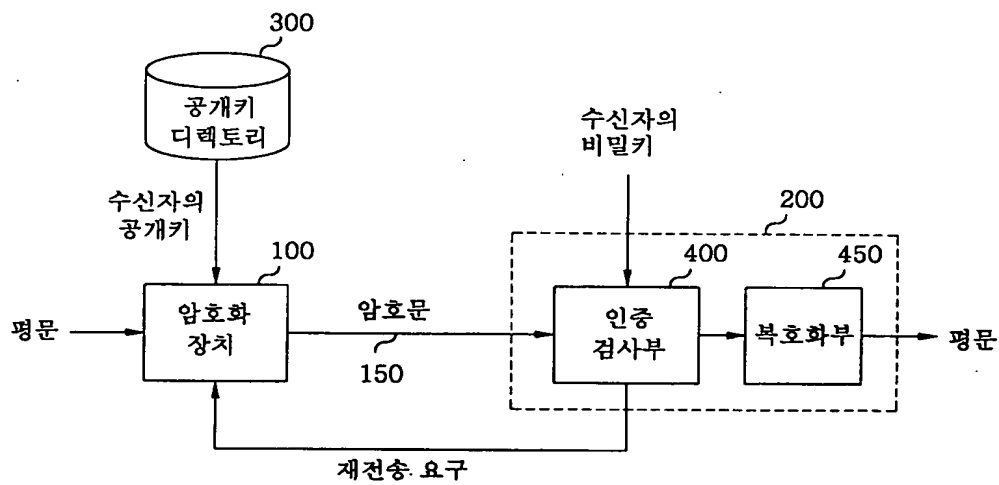
상기 검증값 t에서 뒷부분에 연결된 k_1 길이의 난수를 제거하고, k_0 길이의 평문 m을 복원하는 단계를 구비하는 것을 특징으로 하는 계산적 디피-헬만 가정에 기반하는 안전성이 증명가능한 공개키 암호화 방법.

【도면】

【도 1】



【도 2】



【도 3】

